9

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/404,547	09/24/1999	TAKESHI SAITO	0039-7378-2R	8485

22850 7590 02/11/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
TODD, GREGORY G	
ART UNIT	PAPER NUMBER
2157	

DATE MAILED: 02/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/404,547	**Applicant(s)** SAITO ET AL.
	Examiner Gregory G Todd	**Art Unit** 2157

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *05/07/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This is a fourth office action in response to applicant's request for reconsideration filed, 07 September 2004, of application filed, with the above serial number, on 24 September 1999 in which no claims have been amended. Claims 1-2, and 4-19 are therefore pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 4-11, and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams, Jr. et al (hereinafter "Adams", 5,640,456) in view of Sato (hereinafter "Sato", Philips) and further in view of Hitachi, Ltd. (hereinafter "Hitachi", 5C Digital Transmission Content Protection White Paper).

As per Claim 1, Adams discloses a relay device wherein Adams discloses:

- a first interface unit (port) connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit (port) connected to a second network (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a proxy configuration unit for disclosing a device/service/sub-unit on the second network as an own (transparent; It is interpreted by the office that disclosing a device/service/sub-unit on a network as an own device/service/sub-unit, as acting transparent to a different network) device/service/sub-unit provided on the relay device with respect to a first network side (at least col. 4, lines 37-39);

- a control command reception unit (control terminal) for receiving control command signals destined to the own device/service/sub-unit from the first network side (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a control command transmission unit (control terminal) for transmitting signals corresponding to the control command signals received by the control command reception unit, to the device/service/sub-unit on the second network (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a contents protection information reception unit (part of the downstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for receiving contents protection information (header characters with encryption/decryption information) destined to the own device/service/sub-unit, from a device on the first network (at least col. 6, lines 21-29; col. 4, lines 40-52);

- a contents protection information transfer unit (part of the upstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for transferring the contents protection information (header characters with encryption/decryption information) received by the contents protection information reception unit to the device/service/sub-unit on the second network, without making any change (passed through without modification) in the contents protection information (at least col. 6, lines 21-29; col. 4, lines 40-52);

Adams fails to disclose the first and second network operating under different protocols. However, the use and advantages for using such communication is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Sato. Sato discloses a virtual proxy node doing interpretation between two networks operating under different protocols (at least pp. 4-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of Sato's conversion and interpretation techniques between two networks, such as a 1394 and 802.11 networks, so that one network of devices operating under one protocol can communicate with another network using another protocol, as this is simply acting as a gateway (Adams Fig. 4) in much the same manner as Adams uses a gateway to communicate from the LAN to other protocols on his external network.

Adams and Sato, hereinafter "the combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the combination's system as this would enhance the combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further the two networks of Sato commonly operate under such contents protection schemes, such as WEP on a 802.11 network and DTCP on a 1394 network for example, and it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 2, Adams discloses a relay device wherein Adams discloses:

- a first interface unit; connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own (transparent) device/service/sub-unit provided on the relay device with respect to respective another network (at least col. 4, lines 37-39);

- a control command reception unit (control terminal) for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a control command transmission unit (control terminal) for transmitting signals corresponding to the control command signals received by the control command reception unit, to each device/service/sub-unit on another network different from said one network (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a contents protection information reception unit (part of the upstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for receiving contents protection information destined to the own device/service/sub-unit: from a device on the first network or the second network (at least col. 6, lines 21-29; col. 4, lines 40-52);

- a contents protection information transfer unit (part of the upstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for transferring the contents protection information received by the contents protection information reception unit to said each device/service/sub-unit on said another network, without making any change (passed through without modification) in the contents protection information (at least col. 6, lines 21-29; col. 4, lines 40-52);

a contents reception unit for receiving contents (data portion) destined to the own device/service/sub-unit from a device on the first network or the second network (see col. 4, lines 30-32, 40-46; col. 2, lines 25-40);

a contents transfer unit for transferring the contents (data portion) received by the contents reception unit to said each device/service/sub-unit on said another network, without making any change (passed through) in the contents (see col. 4, lines 30-32, 40-46; col. 2, lines 25-40).

Adams fails to disclose the first and second network operating under different protocols. However, the use and advantages for using such communication is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Sato. Sato discloses a virtual proxy node doing interpretation between two networks operating under different protocols (at least pp. 4-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of Sato's conversion and interpretation techniques between two networks, such as a 1394 and 802.11 networks, so that one network of devices operating under one protocol can communicate with another network using another protocol, as this is simply acting as a gateway (Adams Fig. 4) in much the same manner as Adams uses a gateway to communicate from the LAN to other protocols on his external network.

Adams and Sato, hereinafter "the combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the combination's system as this would enhance the combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further the two networks of Sato commonly operate under such contents protection schemes, such as WEP on a 802.11 network and DTCP on a 1394 network for example, and it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 4, Adams discloses a relay device wherein Adams discloses:

- a configuration information reception unit for receiving configuration information (option bit) from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an authentication format (indicate that data characters are encrypted) for said one device/service/sub-unit (at least col. 6, lines 3-5, 25-29);

- a configuration recognition unit for recognizing (compares) a configuration (information extracted from header according to key list) of said one device/service/sub-unit according to the configuration information (option bit in header) received by the configuration information reception unit (at least col. 6, lines 3-5, 11-16, 25-29).

As per claim 5, Adams discloses a relay device wherein Adams discloses:

- a first interface unit connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (wherein 1394 bus is referred to as another network) (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own (transparent) device/service/sub-unit provided on the relay device with respect to respective another network side (at least col. 4, lines 37-39);

- a control command reception unit (control terminal) for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a control command transmission unit (control terminal) for transmitting signals corresponding to the control command signals received by the control command reception unit, to said each device/service/sub-unit on another network different from said one network (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network (downstream network port) (at least col. 6, lines 6-16, 21-29);

- a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network (upstream network port) (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);

- a contents reception unit for receiving contents (data) destined to the own device/service/sub-unit and encrypted according to one of the first and second contents protection units (at least col. 6, lines 6-16, 21-29);

- a contents transfer unit for transferring the contents (data) received by the contents reception unit to said each device/service/sub-unit on said another network, by encrypting the contents according to another one of the first and second contents protection units (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11).

Adams fails to disclose the first and second network operating under different protocols. However, the use and advantages for using such communication is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Sato. Sato discloses a virtual proxy node doing interpretation between two networks operating under different protocols (at least pp. 4-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of Sato's conversion and interpretation techniques between two networks, such as a 1394 and 802.11 networks, so that one network of devices operating under one protocol can communicate with another network using another protocol, as this is simply acting as a gateway (Adams Fig. 4) in much the same manner as Adams uses a gateway to communicate from the LAN to other protocols on his external network.

Adams and Sato, hereinafter "the combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the combination's system as this would enhance the combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further the two networks of Sato commonly operate under such contents protection schemes, such as WEP on a 802.11 network and DTCP on a 1394 network for example, and it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 6, Adams discloses a relay device wherein Adams discloses:

- the first contents protection unit and the second contents protection unit use identical encryption schemes based on different keys (the same encryption hardware is used with a key list for different keys and headers) (at least col. 4, lines 40-52).

As per claim 7, Adams discloses a relay device wherein Adams discloses:

- a contents reception unit and contents transmission unit (communications ports) sealed within a single LSI (microprocessor) (at least col. 5, lines 21-27).

As per claim 8, Adams discloses a relay device wherein Adams discloses:

- a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical (transferred header containing encryption information) (at least col. 6 line 65 - col. 7 line 11; col. 5 line 65 - col. 6 line 5).

As per claim 9, Adams discloses a relay device wherein Adams discloses:

- the contents protection procedure (encryption) in said another one of the first and second contents protection units carried out in units of contents/services/sub-units (packets), using a prescribed key information (header) (at least col. 5 line 61 - col. 6 line 11).

As per claim 10, Adams discloses a relay device wherein Adams discloses:

- a configuration information reception unit for receiving a configuration information (header) from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an authentication format (indicate that data characters are encrypted) for said one device/service/sub-unit (at least col. 6, lines 3-5, 11-16, 25-29);

- a configuration recognition unit for recognizing (matching criteria) a configuration of said one device/service/sub-unit according to the configuration information received by the configuration information reception unit (at least col. 6, lines 3-5, 11-16, 25-29).

As per claim 11, Adams discloses a relay device wherein Adams discloses:

- a first interface unit connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (wherein 1394 bus is referred to as another network) (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network (downstream network port) (at least col. 6, lines 6-16, 21-29);

- a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network (upstream network port) (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);

- a contents reception unit for receiving contents (data) destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second network (at least col. 6, lines 6-16, 21-29);

- a contents transmission unit for transmitting the contents (data) received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);

- wherein a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical (transferred header containing identical encryption information) (at least col. 6 line 65 - col. 7 line 11; col. 5 line 65 - col. 6 line 5).

Adams fails to disclose the first and second network operating under different protocols. However, the use and advantages for using such communication is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Sato. Sato discloses a virtual proxy node doing interpretation between two networks operating under different protocols (at least pp. 4-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of Sato's conversion and interpretation techniques between two networks, such as a 1394 and 802.11 networks, so that one network of devices operating under one protocol can communicate with another network using another protocol, as this is simply acting as a gateway (Adams Fig. 4) in much the same manner as Adams uses a gateway to communicate from the LAN to other protocols on his external network.

Adams and Sato, hereinafter "the combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the combination's system as this would enhance the combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further the two networks of Sato commonly operate under such contents protection schemes, such as WEP on a 802.11 network and DTCP on a 1394 network for example, and it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 17, Adams discloses a relay device wherein Adams discloses:

- a first interface unit; connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (wherein 1394 bus is referred to as another network) (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a contents reception unit for receiving encrypted data containing contents from the first interface unit (at least col. 6, lines 6-29);

- a decryption unit for decrypting the encrypted data received by the contents reception unit, by using a contents protection key provided by the first copy protection processing unit, to obtain decrypted data (at least col. 7, lines 19-33);

- a conversion unit for converting the decrypted data into converted data in another coding format (at least col. 6, lines 6-29);

- an encryption unit for encrypting the converted data (see below), by using a contents protection key (compare header information with key list) provided by the second copy protection processing unit, to obtain re-encrypted data (at least col. 6, lines 6-16);

- a contents transmission unit for transferring the re-encrypted data to the second interface unit (at least col. 6 line 65 - col. 7 line 11).

Adams fails to disclose the first and second network operating under different protocols. However, the use and advantages for using such communication is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Sato. Sato discloses a virtual proxy node doing interpretation between two networks operating under different protocols (at least pp. 4-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of Sato's conversion and interpretation techniques between two networks, such as a 1394 and 802.11 networks, so that one network of devices operating under one protocol can communicate with another network using another protocol, as this is simply acting as a gateway (Adams Fig. 4) in much the same manner as Adams uses a gateway to communicate from the LAN to other protocols on his external network.

Adams and Sato, hereinafter "the combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the combination's system as this would enhance the combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further the two networks of Sato commonly operate under such contents protection schemes, such as WEP on a 802.11 network and DTCP on a 1394 network for example, and it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 18, Adams discloses a relay device wherein Adams discloses:

- a proxy configuration unit for disclosing one device/service/sub-unit on the second network as one own (transparent) device/service/sub-unit provided on the relay device with respect to a first network side (at least col. 4, lines 37-39), and transmitting to said one device/service/sub-unit on the second network an information having a content (data) according to information (header) destined to said one own device/service/sub-unit that is received from a device on the first network side (transmit packet from first network to second network (downstream)) (see Fig. 7; at least col. 7, lines 51-54), while also disclosing another device/service/sub-unit on the first network as another own device/service/sub-unit provided on the relay device with respect to a second network side (the device is transparent to both sides; It is implied that disclosing a device/service/sub-unit on a network as an own device/service/sub-unit is equivalent to acting transparent to a different network) (at least col. 4, lines 26-39), and transmitting to said another device/service/sub-unit on the first network an information (header) having a content (data) according to information destined to said another own device/service/sub-unit that is received from a device on the second network side (transmit packet from second network to first network (upstream)) (see Fig. 7; at least col. 7, lines 8-12);

- when the prescribed contents protection procedure between a device on one network among the first and second networks and a device/service/sub-unit on another network among the first and second networks is to be carried out, the proxy configuration unit carries out the prescribed contents protection procedure with the device on said one network by using one of the first and second copy protection processing units, while carrying out the prescribed contents protection procedure with the device/service/sub-unit on said another network by using another one of the first and second copy protection processing units (the contents protection procedure (encryption) is carried out between a device (computer) on first network and another device (computer) on another network) (at least col. 4, lines 37-59).

As per claim 19, Adams discloses a relay device wherein Adams discloses:

- a first interface unit connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network (downstream network port) (at least col. 6, lines 6-16, 21-29);

- a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network (upstream network port) (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);

- a contents reception unit for receiving contents (data) destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second networks (at least col. 6, lines 6-16, 21-29);

- a contents transmission unit for transmitting the contents (data) received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11).

Adams fails to disclose the first and second network operating under different protocols. However, the use and advantages for using such communication is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Sato. Sato discloses a virtual proxy node doing interpretation between two networks operating under different protocols (at least pp. 4-6). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the use of Sato's conversion and interpretation techniques between two networks, such as a 1394 and 802.11 networks, so that one network of devices operating under one protocol can communicate with another network using another protocol, as this is simply acting as a gateway (Adams Fig. 4) in much the same manner as Adams uses a gateway to communicate from the LAN to other protocols on his external network.

Adams and Sato, hereinafter "the combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the combination's system as this would enhance the combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further the two networks of Sato commonly operate under such contents protection schemes, such as WEP on a 802.11 network and DTCP on a 1394 network for example, and it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

4. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams, Jr. et al (hereinafter "Adams", 5,640,456) in view of Perlman (hereinafter "Perlman", 5,175,765) and further in view of Hitachi, Ltd. (hereinafter "Hitachi", 5C Digital Transmission Content Protection White Paper).

As per Claim 12, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (mechanism to maintain list of keys for sites so as to change key for respective site) with respect to another device/service/sub-unit on the network (at least col. 4, lines 40-52);

- a contents transmission unit for transmitting encrypted contents to which an address of the communication device is attached, either through a virtual channel on the network or by further attaching an identifier by which the encrypted contents can be uniquely identified by the communication device, to another device on the network (at least col. 6, lines 21-29, 17-20; col. 6 line 65 - col. 7 line 11);

Adams fails to disclose a reception unit for receiving a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, from said another device on the network, or a notification unit for notifying (transmitting to) a service/sub-unit/plug that is transferring the encrypted contents, to said another device on the network in response to the query.

However, the use and advantages for querying over a network is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Perlman (at least col. 14, lines 38-49). Perlman discloses querying nodes from a site on the network and further, the nodes responding back from the query. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the ability to query into the device from Adams because this would ensure and detect that no packets (contents) are being lost in the communication path and that there is a stable, fault-free connection between the device and a node on one of the networks, especially when first setting up the device between the two networks.

Adams and Perlman, hereinafter "the 2nd combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the 2nd combination's system as this would enhance the 2nd combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further, it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 13, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (encryption) with respect to another device/service/sub-unit on the network (at least col. 4, lines 40-52);

- a contents reception unit for receiving encrypted contents to which an address of another device on the network is attached, either through a virtual channel on the network or in a form having an identifier by which the encrypted contents can be uniquely identified by said another device further attached thereto, from said another device (at least col. 6, lines 6-29);

Adams fails to disclose a transmission unit for transmitting a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, to said another device on the network, or a reception unit for receiving a notification regarding a service/sub-unit/plug that is transferring the encrypted contents, from said another device in response to the query.

However, the use and advantages for querying over a network is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Perlman (at least col. 14, lines 38-49). Perlman discloses querying nodes from a site on the network and further, the nodes responding back from the query. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the ability to query into the device from Adams because this would ensure and detect that no packets (contents) are being lost in the communication path and that there is a stable, fault-free connection between the device and a node on one of the networks, especially when first setting up the device between the two networks.

Adams and Perlman, hereinafter "the 2nd combination", fail to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into the 2nd combination's system as this would enhance the 2nd combination's system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further, it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

5. Claims 14-16 and are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams, Jr. et al (hereinafter "Adams", USPN 5,640,456) in view of Hitachi, Ltd. (hereinafter "Hitachi", 5C Digital Transmission Content Protection White Paper).

As per claim 14, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a contents transfer unit for transmitting or receiving encrypted contents with respect to another device on the network, through a flow identified by a set of a source address, a source port, a destination address, and a destination port (at least col. 4, lines 40-44; col. 5 line 65 - col. 6 line 5; col. 6, lines 17-20);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (encryption & plurality of keys for handling the packet) with respect to said another device, using a prescribed logical port, in units of the flow (encrypt data using a key from a key list)(at least col. 4, lines 40-52; col. 6, lines 21-29).

Adams fails to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into Adams' system as this would enhance Adams' system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further, it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

As per claim 15, Adams discloses a communication device wherein Adams discloses:

- an identifier of the flow is attached (in header) to information (data) exchanged in at least a part of procedures included in the prescribed contents protection procedure (at least col. 6 line 65 - col. 7 line 2).

As per claim 16, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (encryption) with respect to another device on the network (at least col. 4, lines 40-52);

- a contents transmission and reception unit for transmitting or receiving encrypted contents to which an address of a transmitting side device is attached, either through a virtual channel on the network or in a form having an identifier by which the encrypted contents can be uniquely identified by said, transmitting side device further attached thereto, with respect to said another device (at least col. 6, lines 6-29; col. 6 line 65 - col. 7 line 11);

- wherein at least one of an identifier of a service, a sub-unit, a virtual channel, or a plug (various network layers) that carries out exchange of the encrypted contents, and an identifier (header) by which the encrypted contents can be uniquely identified by said transmitting side device, is attached to information (data) exchanged in at least a part of procedures included in the prescribed contents protection procedure (encryption) (at least col. 5 line 61 - col. 6 line 5).

Adams fails to disclose carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network. However, the use and advantages for using such a authentication procedure is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of

Hitachi. Hitachi discloses digital content protection such as authentication and key-exchange over network such as a 1394 network (at least pp. 1-2, 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Hitachi's content protection procedure into Adams' system as this would enhance Adams' system to be secure as inter-network security is a very important concept that is commonly placed on many networks with different protocols, and it is obvious for two different networks to communicate with one another to authenticate communication between each device on each network for obvious verification purposes. Further, it would have been obvious for Adams' network offering encryption and decryption along with an authentication procedure as this would ensure that the contents received by a device are decrypted only if authenticated with the source as network security is a rising concern.

Response to Arguments

6. Applicant's arguments filed 07 September 2004 have been fully considered but they are not persuasive.

Applicants argue, in substance, that a) Adams fails to teach any contents protection procedure including at least an authentication and/or a key exchange; b) Adams fails to suggest any relay device that selectively relays only the contents protection information transparently; c) Adams fails to teach a relay device that carries out contents protection procedures separately and re-encrypts the contents at the time of the contents transfer; d) Perlman fails to teach any query and reply regarding a service/sub-unit/plug that is transferring contents, particularly to ascertain which service/sub-unit/plug is transferring the encrypted contents; e) Adams fails to teach a flow; and f) Adams fails to teach any identifier of a service, a sub-unit, a virtual channel, or a plug for uniquely identifying encrypted contents.

In reply to a); In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Hitachi is relied on for teaching contents protection procedure including at least an authentication and/or a key exchange.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Adams is using contents protection in the form of encryption and decryption and Hitachi is relied on only for teaching contents protection procedure to further include an authentication and/or a key exchange.

In reply to b); In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., transparently relaying contents protection information, without making any change, while relaying control command signals non-transparently) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In reply to c); In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., relay device carrying out the contents protection procedures separately) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Further, Adams teaches encrypting the contents of the packets prior to transfer in the cited portions (see col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11).

In reply to d); As previously discussed, Perlman teaches basic querying for packet reception and responding with a confirmation (at least col. 14, lines 38-49). This reads on the claim of the reception unit receiving a query from another device on the network and notification unit for responding to the query. Combined with Adams' use of encryption of contents for transmission over the network, Perlman and Adams teach the basic principle of such an ACK and receipts type service for such querying.

In reply to e); Adams teaches transferring contents according to header information (this information containing source/dest port/address) (at least col. 6, lines 6-20) and using masking to determine which sub-network/network. It was well known in the art at the time the invention was made that a packet header contains a source/dest port/addresses as Adams teaches (at least col. 5, lines 65-67) and thus Adams clearly transfers data according to the header information. Such a flow, as the claims state, being identified by a set of a source address and port as well as a destination address and port, thus Adams clearly teaches such a "flow".

In reply to f); Adams teaches various network layers inserting unique information into the packets to include an option bit for identifying and indicating to the receiving node, the status of the encryption of the contents prior to transfer of the contents (see col. 5 line 61 - col. 6 line 5). Thus Applicants arguments are not persuasive and the rejection stands.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Newly cited Botham, Jr. et al in addition to previously cited Kimura et al, Zhang, Stewart, Shimbo et al, Shimadoi et al, Nomura, Lea, Vu, Daniels et al, Templin et al, Kimura et al, Sharpe, and Brewer are cited for disclosing pertinent information related to the claimed invention. Applicants are requested to consider the prior art reference for relevant teachings when responding to this office action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory G Todd whose telephone number is (571)272-4011. The examiner can normally be reached on Monday - Friday 9:00am-6:00pm w/ first Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571)272-4001. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Gregory Todd
Patent Examiner
Technology Center 2100

MARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100